Exhibit 26

AN HOUR AGO AN HOUR AGO

2020 CANDIDATE SLIDESHOWS

DECEMBER 15, 2020 / 9:08 PM / UPDATED 2 MONTHS AGO

Hackers used SolarWinds' dominance against it in sprawling spy campaign

By Raphael Satter, Christopher Bing, Joseph Menn

WASHINGTON (Reuters) - On an earnings call two months ago, SolarWinds Chief Executive Kevin Thompson touted how far the company had gone during his 11 years at the helm.

FILE PHOTO: Optical fibre cables are seen in a telephone exchange in Rome, Italy December 20, 2013. REUTERS/Alessandro Bianchi

NOW READING Hackers used SolarWinds' dominance against it in sprawling spy campaign

Georgia Republican Perdue will not seek Senate return in 2022
AN HOUR AGO

Former House security chief denies 'optics' dictated decisi...
AN HOUR AGO

“We don’t think anyone else in the market is really even close in terms of the breadth of coverage we have,” he said. “We manage everyone’s network gear.”

Now that dominance has become a liability - an example of how the workhorse software that helps glue organizations together can turn toxic when it is subverted by sophisticated hackers.

On Monday, SolarWinds confirmed that Orion - its flagship network management software - had served as the unwitting conduit for a sprawling international cyberespionage operation. The hackers inserted malicious code into Orion software updates pushed out to nearly 18,000 customers.

And while the number of affected organizations is thought to be much more modest, the hackers have already parlayed their access into consequential breaches at the U.S. Treasury and Department of Commerce.

Three people familiar with the investigation have told Reuters that Russia is a top suspect, although others familiar with the inquiry have said it is still too early to tell.

A SolarWinds representative, Ryan Toohey, said he would not be making executives available for comment. He did not provide on-the-record answers to questions sent via email.

In a statement issued Sunday, the company said “we strive to implement and maintain appropriate administrative, physical, and technical safeguards, security processes, procedures, and standards designed to protect our customers.”

Cybersecurity experts are still struggling to understand the scope of the damage.

The malicious updates - sent between March and June, when America was hunkering down to weather the first wave of coronavirus infections - was “perfect timing for a perfect storm,” said

NOW READING Hackers used SolarWinds' dominance against it in sprawling spy campaign

Georgia Republican Perdue will not seek Senate return in 2022
AN HOUR AGO

Former House security chief denies 'optics' dictated decisi...
AN HOUR AGO

“We may not know the true impact for many months, if not more – if not ever,” she said.

The impact on SolarWinds was more immediate. U.S. officials ordered anyone running Orion to immediately disconnect it. The company’s stock has tumbled more than 23% from $23.50 on Friday - before Reuters broke the news of the breach - to $18.06 on Tuesday.

SolarWinds’ security, meanwhile, has come under new scrutiny.

In one previously unreported issue, multiple criminals have offered to sell access to SolarWinds’ computers through underground forums, according to two researchers who separately had access to those forums.

NOW READING Hackers used SolarWinds' dominance against it in sprawling spy campaign

Georgia Republican Perdue will not seek Senate return in 2022

AN HOUR AGO

Former House security chief denies 'optics' dictated decisi...

AN HOUR AGO

Security researcher Vinoth Kumar told Reuters that, last year, he alerted the company that anyone could access SolarWinds' update server by using the password "solarwinds123"

"This could have been done by any attacker, easily," Kumar said.

Neither the password nor the stolen access is considered the most likely source of the current intrusion, researchers said.

Others - including Kyle Hanslovan, the cofounder of Maryland-based cybersecurity company Huntress - noticed that, days after SolarWinds realized their software had been compromised, the malicious updates were still available for download.

The firm has long mooted the idea of spin-off of its managed service provider business and on Dec. 9 announced that Thompson would be replaced by Sudhakar Ramakrishna, the former chief executive of Pulse Secure. Three weeks ago, SolarWinds posted a job ad seeking a new vice president for security; the position is still listed as open.

Thompson and Ramakrishna could not be reached for comment.

Reporting by Raphael Satter and Christopher Bing. Jack Stubbs contributed reporting from London; Editing by Lisa Shumaker

Our Standards: The Thomson Reuters Trust Principles.

MORE FROM REUTERS